PRIVACY IMPACT ASSESSMENT (PIA)

For the

mCare Bidirectional Secure Messaging System
US Army Medical Command - DHP Funded Application

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☒	**New Electronic Collection**
☐	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☐	**Yes, DITPR**	Enter DITPR System Identification Number	
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☒	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier A0040-66b DASG

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C 3013, Secretary of the Army; 10 U.S.C. 1071-1085, Medical and Dental Care; 50 U.S.C. Supplement IV, Appendix 454, as amended, Persons liable for training and service; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; 10 U.S.C. 1097a and 1097b TRICARE Prime and TRICARE Program; 10 U.S.C. 1079, Contracts for Medical Care for Spouses and Children; 10 U.S.C. 1079a, CHAMPUS; 10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; E.O. 9397 (SSN); DoD "Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoD Directive 6040.37, Confidentiality of Medical Quality Assurance (QA) Records, DoD 6010.8-R, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); Army Regulation 40-66, Medical Record Administration and Healthcare Documentation.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The mCare is a pilot stage, MEDCOM initiative. It is a bidirectional secure messaging system that allows Wounded Warriors to receive and communicate with their case management team members through their personal cell phones. This secure messaging system reminds patients of their upcoming appointments and also conveys other specific information relevant to their unique status as Wounded Warriors. The secure mCare application on the patient's phone allows them to respond to their case management team reminders and other secure messages in a manner that allows the care team to track patient progress through a secure web site, and when needed, receive e-mail alerts to engage the patient in an immediate fashion. The mCare system is an augment to other forms of patient outreach, and not a replacement for direct or telephonic contact by the care team.

The mCare system collects the following PII: patient's name, personal cell phone number, mailing address, marital status, birth date, home phone number, SSN, gender and medical information.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Applicable privacy risks include unauthorized access and unauthorized disclosure of PII. The system only uses information that is needed to provide timely and appropriate secure messaging to the patient as a voluntary service. To ensure that no PII is accessed by unauthorized personnel, all information is encrypted using approved standards. To access the information through the web site, the healthcare team member must have authorized credentials and privileges to view the information. For the patient to access the information from their cell phone, they must enter a personal identification number (PIN) that is only known to them. If the PIN is entered incorrectly on multiple attempts, the application is locked and will require the healthcare team to reset the account with a new authorization code and have the patient select a new PIN.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. The PII will be shared with nurse case managers and physicians within the assigned medical treatment facility using this application

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Some healthcare personnel are employed in a contractual basis. There are clauses in their contracts requiring compliance with the Privacy Act and Health Insurance

Portability and Accountability Act (HIPAA)

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individuals who volunteer to participate in the mCare project receive a Privacy Advisory. Individuals who object to the collection of their PII will not be enrolled in the mCare project.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Individuals who volunteer to participate in the mCare project receive a Privacy Advisory. Individuals who do not consent to the specifics uses of their PII object will not be enrolled in the mCare project.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. **What information is provided to an individual when asked to provide PII data?** Indicate all that apply.

☐	**Privacy Act Statement**	☒	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with the request for information solicited during your enrollment into the mCare project.

Accordingly, pursuant to the requirements of the Act, please be advised that (I) the authority for the collection of this data is 35 U.S. C. §§ 1.6 and 31, (ii) furnishing of the information solicited is voluntary, and (iii) the principal purpose for which the data will be used is to maintain current information relating to your ability to receive and send secure messages through your personal cell phone about your healthcare needs. If you do not furnish the requested information, you will not be enrolled in the mCare project.

The information is accessible to US Army healthcare personnel who are assigned oversight duties for your healthcare, mCare data managers who maintain the operations for secure messaging, and system analysts who produce summary descriptive statistics and analytical studies about the performance of the mCare system. All of these personnel sign confidentiality agreements and other legally binding documents that prohibit the disclosure of personal information. Furthermore, they are trained on the management of personal information.

Your information will not be sold or transferred to any other commercial or government agency.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

E-mail Confirmation Report

Date/Time	:	OCT-31-2011 07:03AM MON
Fax Number	:	2102218422
Fax Name	:	Xerox Phaser 3635
Model Name	:	Phaser 3635MFP

1. Job Status : Succeeded

2. Job Information

Device Name	:	XRX0000AAB9CC67
Submission Date/Time	:	10-31 07:03AM
Images Scanned	:	5
Size	:	196374 Byte(s)

3. SMTP Server

Address	:	139.232.7.20

4. Message Settings

Subject	:	Scan from a Xerox Phaser MFP
From	:	john.gerzsenye@AMEDD.ARMY.MIL
To	:	john.gerzsenye@amedd.army.mil
		john.gerzsenye@AMEDD.ARMY.MIL